

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method of transporting keys in a quantum cryptographic key distribution (QKD) network, comprising:

exchanging a respective number of secret key bits between nodes of the QKD network using QKD techniques;

determining link metrics associated with quantum cryptographic links of the QKD network based on the respective number of secret key bits exchanged between the nodes of the QKD network;

determining one or more paths for transporting secret keys, ~~using QKD techniques~~, across the QKD network based on the determined link metrics; and

transporting the secret keys across the QKD network using the determined one or more paths.

2. (Original) The method of claim 1, wherein the determining one or more paths comprises:
using a centralized path determination algorithm for determining the one or more paths.

3. (Original) The method of claim 1, wherein the determining one or more paths comprises:
using distributed path determination algorithms for determining the one or more paths.

4. (Original) The method of claim 1, wherein the determining one or more paths for transporting the secret keys across the QKD network comprises:
using a shortest path first algorithm for determining the one or more paths.

5. (Currently amended) The method of claim 1, wherein ~~the~~ determining ~~the~~ one or more paths for transporting the secret keys across the QKD network comprises:
determining multiple disjoint, or partially disjoint, paths for transporting secret keys across the QKD network.

6-11. (Canceled)

12. (Currently amended) A method of determining link metrics of quantum cryptographic links connecting a node to neighboring nodes in a quantum cryptographic key distribution (QKD) network, comprising:

exchanging secret key bits with each of the neighboring nodes using quantum cryptographic mechanisms via the quantum cryptographic links;

determining a respective number of available secret key bits exchanged with ~~the~~ each of the neighboring nodes; and

determining link metrics associated with each of the quantum cryptographic links based on the respective number of secret key bits exchanged with the each of the neighboring nodes.

13. (Original) The method of claim 12, further comprising:
storing the respective secret key bits exchanged with each of the neighboring nodes, and
wherein determining the link metrics associated with each of the quantum cryptographic links
further comprises:
determining a rate of change in a number of the stored respective secret key bits.
14. (Original) The method of claim 12, further comprising:
storing the respective secret key bits exchanged with each of the neighboring nodes, and
wherein determining the link metrics associated with each of the quantum cryptographic links
further comprises:
predicting availability of a number of the stored respective secret key bits.
15. (Original) The method of claim 12, further comprising:
disseminating the link metrics using link state routing protocols.
16. (Original) The method of claim 12, further comprising:
disseminating the link metrics associated with each of the quantum cryptographic links to
the neighboring nodes.
17. (Original) The method of claim 16, further comprising:

disseminating the link metrics associated with each of the quantum cryptographic links to other nodes in the network.

18. (Original) A computer-readable medium containing instructions for controlling at least one processor to perform a method of determining link metrics of quantum cryptographic links connecting a node to neighboring nodes in a quantum cryptographic key distribution (QKD) network, the method comprising:

sharing secret key bits with each of the neighboring nodes using quantum cryptographic mechanisms via quantum cryptographic links;

determining a respective number of secret key bits shared with the each of the neighboring nodes; and

determining link metrics associated with each of the quantum cryptographic links based on the respective number of secret key bits shared with the each of the neighboring nodes.

19. (Currently amended) A quantum cryptographic key distribution node, comprising:
one or more quantum cryptographic link interfaces configured to:

exchange secret key bits with each neighboring node using quantum cryptographic mechanisms via one or more quantum cryptographic links; and

processing logic configured to:

determine a respective number of secret key bits exchanged with the each neighboring node, and

determine link metrics associated with each respective quantum cryptographic link of the one or more quantum cryptographic links based on the respective number of secret key bits exchanged with the ~~each~~ neighboring node.

20. (Currently amended) A system for determining link metrics of quantum cryptographic links connecting a node to neighboring nodes in a quantum cryptographic key distribution (QKD) network, comprising:

means for exchanging secret key bits with each of the neighboring nodes using quantum cryptographic mechanisms via quantum cryptographic links;

means for determining a respective number of secret key bits exchanged with ~~the~~ each of the neighboring nodes; and

means for determining link metrics associated with each respective quantum cryptographic link based on the respective number of secret key bits exchanged with ~~the~~ each of the neighboring nodes.

21. (Original) A method of determining a link metric for each direction along quantum cryptographic links in a quantum cryptographic key distribution (QKD) network, comprising:

exchanging quantities of secret key bits between neighboring nodes in the QKD network using quantum cryptographic mechanisms over the quantum cryptographic links; and

determining link metrics for each direction along each respective quantum cryptographic link of the quantum cryptographic links based on the exchanged quantities of secret key bits.

22. (Original) The method of claim 21, further comprising:
disseminating the link metrics using link state routing protocols.

23. (Original) The method of claim 21, further comprising:
disseminating the link metrics associated with each respective quantum cryptographic link to the neighboring nodes.

24. (Original) The method of claim 23, further comprising:
disseminating the link metrics associated with each respective quantum cryptographic link to other nodes in the network.

25. (Original) A data structure encoded on a computer-readable medium, comprising:
first data identifying a first neighboring node in a quantum cryptographic key distribution (QKD) network;
second data identifying a first number of secret key bits exchanged with the first neighboring node via quantum cryptographic mechanisms; and
third data comprising a link metric associated with a link to the first neighboring node, the link metric being based on the first number of secret key bits exchanged with the first neighboring node.

26. (Currently amended) The data structure of claim 25, further comprising:

fourth data identifying a second neighboring node in a quantum cryptographic key distribution (QKD) network;

fifth data identifying a second number of secret key bits exchanged with the second neighboring node via quantum cryptographic mechanisms; and

sixth data comprising a link metric associated with a link to the second neighboring node, the link metric being based on the second number of secret key bits exchanged with the second neighboring node.

27. (Canceled)